

# Carlitz Rank and Index of Permutation Polynomials

Leyla Işık<sup>1</sup>, Arne Winterhof<sup>2</sup>,

<sup>1</sup> Salzburg University, Hellbrunnerstr. 34, 5020 Salzburg, Austria  
E-mail: leyla.isik@sbg.ac.at

<sup>2</sup> Johann Radon Institute for Computational and Applied Mathematics  
Austrian Academy of Sciences, Altenbergerstr. 69, 4040 Linz, Austria  
E-mail: arne.winterhof@oeaw.ac.at

## Abstract

Carlitz rank and index are two important measures for the complexity of a permutation polynomial  $f(x)$  over the finite field  $\mathbb{F}_q$ . In particular, for cryptographic applications we need both, a high Carlitz rank and a high index. In this article we study the relationship between Carlitz rank  $Crk(f)$  and index  $Ind(f)$ . More precisely, if the permutation polynomial is neither close to a polynomial of the form  $ax$  nor a rational function of the form  $ax^{-1}$ , then we show that  $Crk(f) > q - \max\{3Ind(f), (3q)^{1/2}\}$ . Moreover we show that the permutation polynomial which represents the discrete logarithm guarantees both a large index and a large Carlitz rank.

**Keywords:** Carlitz rank, character sums, cryptography, finite fields, index, invertibility, linearity, permutation polynomials, cyclotomic mappings, discrete logarithm.

**Mathematical Subject Classification:** 11T06, 11T24, 11T41, 11T71.

# 1 Introduction

In 1953, L. Carlitz [2] proved that all permutation polynomials over the finite field  $\mathbb{F}_q$  of order  $q \geq 3$  are compositions of linear polynomials  $ax + b$ ,  $a, b \in \mathbb{F}_q$ ,  $a \neq 0$ , and inversions  $x^{q-2} = \begin{cases} 0, & x = 0, \\ x^{-1}, & x \neq 0, \end{cases}$  see [2] or [5, Theorem 7.18]. Consequently, any permutation of  $\mathbb{F}_q$  can be represented by a polynomial of the form

$$P_n(x) = (\dots((c_0x + c_1)^{q-2} + c_2)^{q-2} \dots + c_n)^{q-2} + c_{n+1}, \quad (1)$$

where  $c_i \neq 0$ , for  $i = 0, 2, \dots, n$ . (Note that  $c_1c_{n+1}$  can be zero.) This representation is not unique and  $n$  is not necessarily minimal. We recall that the *Carlitz rank*  $Crk(f)$  of a permutation polynomial  $f(x)$  over  $\mathbb{F}_q$  is the smallest integer  $n \geq 0$  satisfying  $f(x) = P_n(x)$  for a permutation polynomial  $P_n(x)$  of the form (1). The Carlitz rank was first introduced in [1] and further studied in [3, 4]. For a survey see [10].

In 2009, Aksoy et al. [1] showed

$$Crk(f) \geq q - \deg(f) - 1 \quad \text{if } \deg(f) \geq 2. \quad (2)$$

In [3] Gomez-Perez et al. gave a similar bound for  $Crk(f)$  in terms of the weight  $w(f)$  of  $f(x)$ , that is the number of its nonzero coefficients. If  $f(x) \neq a + bx^{q-2}$ , for all  $a, b \in \mathbb{F}_q$ ,  $b \neq 0$ , then

$$Crk(f) > \frac{q}{w(f) + 2} - 1 \quad \text{if } \deg(f) \geq 2. \quad (3)$$

In this paper, we study the relationship between the Carlitz rank and the least index of a polynomial introduced in [8, 12] as follows.

Let  $\ell$  be a positive divisor of  $q - 1$  and  $\xi$  a primitive element of  $\mathbb{F}_q$ . Then the set of nonzero  $\ell$ th powers

$$C_0 = \left\{ \xi^{j\ell} : j = 0, 1, \dots, \frac{q-1}{\ell} - 1 \right\}$$

is a subgroup of  $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$  of index  $\ell$ . The elements of the factor group  $\mathbb{F}_q^*/C_0$  are the *cyclotomic cosets*

$$C_i = \xi^i C_0, \quad i = 0, 1, \dots, \ell - 1.$$

For any positive integer  $r$  and any  $a_0, a_1, \dots, a_{\ell-1} \in \mathbb{F}_q^*$ , we define the  $r$ -th order cyclotomic mapping  $f_{a_0, a_1, \dots, a_{\ell-1}}^r$  of index  $\ell$  by

$$f_{a_0, a_1, \dots, a_{\ell-1}}^r(x) = \begin{cases} 0 & \text{if } x = 0, \\ a_i x^r & \text{if } x \in C_i, 0 \leq i \leq \ell - 1. \end{cases} \quad (4)$$

For a polynomial  $f(x)$  over  $\mathbb{F}_q$  with  $f(0) = 0$  we denote by  $Ind(f)$  the smallest index  $\ell$  such that  $f(x)$  can be represented in the form (4). The index was introduced in [12] based on [8] and further studied in [6, 11, 13]. The index of  $f(x)$  with  $f(0) \neq 0$  is defined as the index of  $f(x) - f(0)$ . Since  $Crk(f + c)$  is the same as  $Crk(f)$  for any  $c \in \mathbb{F}_q$  we may restrict ourselves to the case  $f(0) = 0$ .

By [12, Theorem 1],  $f_{a_0, a_1, \dots, a_{\ell-1}}^r(x)$  is a permutation of  $\mathbb{F}_q$  if and only if  $\gcd(r, (q-1)/\ell) = 1$  and  $\{a_0, a_1 \xi^r, a_2 \xi^{2r}, \dots, a_{\ell-1} \xi^{(\ell-1)r}\}$  is a system of distinct representatives of  $\mathbb{F}_q^* \setminus C_0$ . In particular,  $f_{a_0, a_1, \dots, a_{\ell-1}}^r(x)$  is a permutation if  $\gcd(r, (q-1)/\ell) = 1$  and all  $a_0, a_1, \dots, a_{\ell-1}$  are in the same cyclotomic coset  $C_i$  of order  $\ell$ .

Now we define two further measures for the unpredictability of a polynomial. The *linearity*  $\mathcal{L}(f)$  of a polynomial  $f(x)$  over  $\mathbb{F}_q[x]$  with  $f(0) = 0$  is

$$\mathcal{L}(f) = \max_{a \in \mathbb{F}_q^*} |\{c \in \mathbb{F}_q : f(c) = ac\}|$$

and the *invertibility*  $\mathcal{I}(f)$  of  $f(x)$  is

$$\mathcal{I}(f) = \max_{c \in \mathbb{F}_q^*} \left| \left\{ x \in \mathbb{F}_q^* : f(x) = \frac{c}{x} \right\} \right|.$$

For cryptographic applications we need unpredictable permutation polynomials, see for example [9]. In particular,  $\mathcal{L}(f)$  and  $\mathcal{I}(f)$  must both be small, and  $Crk(f)$ ,  $\deg(f)$ , and  $w(f)$  must all be large. In Section 3 we prove a relation between  $Crk(f)$  and  $Ind(f)$  of the same flavour as (2) and (3) provided that  $\mathcal{L}(f)$  and  $\mathcal{I}(f)$  are not large. We improve this result for large index  $\ell$  in the special case when the coefficients  $a_0, a_1, \dots, a_{\ell-1}$  in (4) are all in the same cyclotomic coset of index  $\ell$ .

Moreover, in Section 4 we provide an example of a permutation polynomial of small linearity, small invertibility, large degree, large weight, large index and large Carlitz rank. This polynomial represents (up to an additive constant 1) the discrete logarithm of  $\mathbb{F}_p$  for prime  $p$ .

## 2 Preliminary results

Let  $f(x)$  be a permutation polynomial of  $\mathbb{F}_q$ . Then there exist  $\alpha, \beta, \gamma, \delta \in \mathbb{F}_q$  such that

$$f(c) = \frac{\alpha c + \beta}{\gamma c + \delta} \quad \text{for at least } q - Crk(f) \text{ different elements } c \in \mathbb{F}_q, \quad (5)$$

see [10, Section 2]. We may assume

$$\alpha\delta \neq \beta\gamma$$

since otherwise  $\frac{\alpha x + \beta}{\gamma x + \delta}$  is constant and thus  $Crk(f) \geq q - 1$ .

Note that if  $\beta = \gamma = 0$ , then  $f(c) = \frac{\alpha}{\delta}c$  for at least  $q - Crk(f)$  different elements  $c \in \mathbb{F}_q$  and thus

$$Crk(f) \geq q - \mathcal{L}(f) \quad \text{if } \beta = \gamma = 0. \quad (6)$$

If  $\alpha = \delta = 0$ , then  $f(c) = \frac{\beta}{\gamma c}$  for at least  $q - Crk(f)$  different  $c \in \mathbb{F}_q$  and thus

$$Crk(f) \geq q - \mathcal{I}(f) \quad \text{if } \alpha = \delta = 0. \quad (7)$$

Now let  $f(x)$  be an  $r$ -th order cyclotomic mapping permutation polynomial of index  $\ell$  as defined in (4) and assume that  $\beta \neq 0$  or  $\gamma \neq 0$  or  $r \geq 2$ . Then (5) has at most  $(r + 1)\ell$  solutions and we get

$$Crk(f) \geq q - (r + 1)Ind(f), \quad \beta \neq 0 \text{ or } \gamma \neq 0. \quad (8)$$

If  $\alpha \neq 0$  or  $\delta \neq 0$  or  $r \leq q - 3$ , then

$$a_i c^r = \frac{\alpha c + \beta}{\gamma c + \delta}$$

or equivalently

$$\gamma c + \delta = a_i^{-1}(\alpha c^{q-r} + \beta c^{q-r-1})$$

has at most  $q - r$  solutions and thus

$$Crk(f) \geq q - (q - r)Ind(f), \quad \alpha \neq 0 \text{ or } \gamma \neq 0. \quad (9)$$

Collecting (6), (7), (8), (9) we get

$$Crk(f) \geq q - \max \left\{ \min\{r + 1, q - r\}Ind(f), \mathcal{L}(f), \mathcal{I}(f) \right\}.$$

Our goal is to find a similar bound which does not depend on  $r$ .

### 3 Main results

**Theorem 1.** *For any permutation polynomial  $f(x)$  we have*

$$Crk(f) > q - \max \{3Ind(f), (3q)^{1/2}, \mathcal{L}(f), \mathcal{I}(f)\}.$$

*Proof.* By (6) and (7) we may restrict ourselves to the case when neither  $\beta = \gamma = 0$  nor  $\alpha = \delta = 0$ .

Put  $\ell = Ind(f)$ , that is,  $f(x)$  is of the form (4).

Let  $N$  be the number of solutions  $c \in \mathbb{F}_q$  of

$$f(c) = \frac{\alpha c + \beta}{\gamma c + \delta}.$$

Put  $R(c) = \frac{\alpha c + \beta}{\gamma c + \delta}$  and note that  $N$  is the cardinality of the set

$$\mathcal{N} = \{(\xi^i, y) : i = 0, 1, \dots, \ell - 1, y \in C_0 \text{ with } a_i \xi^{ir} y^r = R(\xi^i y)\}.$$

Let  $N_i$  be the contribution to  $N$  for fixed  $i = 0, 1, \dots, \ell - 1$ . Then by the Cauchy-Schwarz inequality we have

$$N^2 = \left( \sum_{i=0}^{\ell-1} N_i \right)^2 \leq \ell M,$$

where

$$M = \sum_{i=0}^{\ell-1} N_i^2.$$

Now we have

$$M = \left| \{(\xi^i, y, z) : i = 0, 1, \dots, \ell - 1, y, z \in C_0 \text{ with } a_i \xi^{ir} y^r = R(\xi^i y) \text{ and } a_i \xi^{ir} y^r z^r = R(\xi^i y z)\} \right|.$$

Then

$$R(\xi^i y z) = a_i \xi^{ir} y^r z^r = z^r R(\xi^i y),$$

that is,

$$\frac{\alpha \xi^i y z + \beta}{\gamma \xi^i y z + \delta} = z^r \frac{\alpha \xi^i y + \beta}{\gamma \xi^i y + \delta},$$

which implies

$$\alpha \gamma \xi^{2i} y^2 z + (\alpha \delta z + \beta \gamma) \xi^i y + \beta \delta = \alpha \gamma \xi^{2i} y^2 z^{r+1} + (\alpha \delta + \beta \gamma z) \xi^i y z^r + \beta \delta z^r. \quad (10)$$

First we consider the case  $\alpha\gamma \neq 0$ . We note that  $z^{r+1} = z$  implies  $z = 1$  since  $z \in C_0$  and  $\gcd(r, \frac{q-1}{\ell}) = 1$ . Therefore for the case  $z = 1$ , (10) is true for all  $N$  pairs  $(\xi^i, y) \in \mathcal{N}$ . For each  $z \neq 1$  there are at most two solutions  $\xi^i y$ . Thus

$$M \leq N + 2 \left( \frac{q-1}{\ell} - 1 \right),$$

which implies

$$N^2 < \ell N + 2q \leq 3 \max\{\ell N, q\}.$$

Hence we get

$$N < \max\{3\ell, (3q)^{1/2}\}. \quad (11)$$

Now we suppose that  $\alpha\gamma = 0$ . First consider the case  $\alpha = 0$ . Note that here  $\delta \neq 0$  and  $\beta\gamma \neq 0$ . Then we have  $\beta\gamma\xi^i y + \beta\delta = \beta\gamma\xi^i y z^{r+1} + \beta\delta z^r$ . This equation has at most one solution  $\xi^i y$  for each  $z \neq 1$  and  $N$  solutions if  $z = 1$ . Therefore

$$M \leq N + \left( \frac{q-1}{\ell} - 1 \right),$$

which implies

$$N < \max\{2\ell, (2q)^{1/2}\}. \quad (12)$$

The case  $\gamma = 0$  is similar. Now the result follows by (5), (11) and (12).  $\square$

Remark. [8, Theorem 1] implies that  $\deg(f) \geq \frac{q-1}{\text{Ind}(f)} + 1$  and the right hand side of (2) is at most  $q - \frac{q-1}{\text{Ind}(f)} - 2$ . Hence Theorem 1 improves (2) if  $\max\{\text{Ind}(f), \mathcal{L}(f), \mathcal{I}(f)\} \leq (q/3)^{1/2}$  and (3) if  $\max\{\text{Ind}(f), \mathcal{L}(f), \mathcal{I}(f)\} \leq 2q/9$ .

We note that the following theorem gives a better bound whenever  $\text{Ind}(f) > q^{1/2}$  provided that all coefficients  $a_i$  are in the same cyclotomic coset.

**Theorem 2.** *Let  $f(x)$  be a permutation polynomial of  $\mathbb{F}_q$  of index  $\ell$  of the form (4) with all  $a_i$  in the same coset of order  $\ell$ . Then*

$$\text{Crk}(f) \geq q - \max\{3q^{1/2}, \mathcal{L}(f), \mathcal{I}(f)\}.$$

*Proof.* Since otherwise the result follows from Theorem 1 we may restrict ourselves to the case  $\text{Ind}(f) > q^{1/2}$  as well as to the case that neither  $\alpha = \delta = 0$  nor  $\beta = \gamma = 0$  by (6) and (7).

Let  $\chi$  be a character of order  $\ell$ , then  $\chi(a_i) = \rho$  for all  $i = 0, 1, \dots, \ell - 1$ . (Note that some of the  $a_i$  can be the same and we can do this also if  $\ell \geq |C_0| =$

$(q-1)/\ell$ , that is,  $\ell > q^{1/2}$ .) Under this condition  $f(x)$  is a permutation and we can estimate the number  $N$  of  $c$  satisfying

$$R(c) = \frac{\alpha c + \beta}{\gamma c + \delta} = f(c). \quad (13)$$

If (13) is true, then we have  $\chi(R(c)) = \chi(c^r)\rho$ . Since

$$\theta(c) = \frac{1}{\ell} \sum_{i=0}^{\ell-1} \left( \chi(\alpha c + \beta) \overline{\chi}(\gamma c + \delta) \overline{\chi}(c^r) \rho^{-1} \right)^i = \begin{cases} 1, & \chi(R(c)) = \chi(c^r)\rho, \\ 0, & \chi(R(c)) \neq \chi(c^r)\rho, \end{cases}$$

for any  $c$  with  $c(\alpha c + \beta)(\gamma c + \delta) \neq 0$ , we have

$$N \leq \sum_{c \in \mathbb{F}_q^* \setminus \{-\beta\alpha^{-1}, -\delta\gamma^{-1}\}} \theta(c),$$

and get

$$\begin{aligned} N &< \frac{1}{\ell} \sum_{i=0}^{\ell-1} \sum_{c \in \mathbb{F}_q} \left( \chi(\alpha c + \beta) \overline{\chi}(\gamma c + \delta) \overline{\chi}(c^r) \rho^{-1} \right)^i \\ &= \frac{q}{\ell} + \max_{i=1,2,\dots,\ell-1} \left| \sum_{c \in \mathbb{F}_q} \left( \chi(\alpha c + \beta) \overline{\chi}(\gamma c + \delta) \overline{\chi}(c^r) \right)^i \right| \leq \frac{q}{\ell} + 2q^{1/2} \leq 3q^{1/2} \end{aligned}$$

by the Weil bound, see for example [5, Theorem 5.41], and the result follows by (5).  $\square$

## 4 The discrete logarithm of $\mathbb{F}_p$

In this section we consider the following permutation over  $\mathbb{F}_p$  where  $p > 2$  is a prime which represents up to +1 the discrete logarithm of  $\mathbb{F}_p$ ,

$$f(\xi^i) = i + 1, \quad i = 0, 1, \dots, p-2, \quad f(0) = 0, \quad (14)$$

where  $\xi$  is again a primitive element of  $\mathbb{F}_p$ . We show that any polynomial  $f(x)$  representing this permutation has large degree, weight, Carlitz rank and index as well as small linearity and invertibility.

**Theorem 3.** *The unique polynomial  $f(x) \in \mathbb{F}_p[x]$  of degree at most  $p - 1$  defined by the property (14) satisfies*

$$\deg(f) = w(f) = p - 2,$$

$$\text{Ind}(f) = p - 1, \quad p > 3,$$

$$\mathcal{L}(f) < (2(p - 2))^{1/2} + 1,$$

$$\mathcal{I}(f) < 2(p - 2)^{1/2} + 1,$$

and

$$\text{Crk}(f) > p - 2(p - 2)^{1/2} - 1.$$

*Proof.* By [7] we have

$$f(c) = \sum_{i=1}^{p-2} (\xi^{-i} - 1)^{-1} c^i, \quad c \in \mathbb{F}_p,$$

and the first result follows.

Next we estimate the index  $\ell$  of  $f(x)$ . Assume  $\ell \leq (p - 1)/3$ . Then there is some  $a \in \mathbb{F}_p^*$  with

$$f(\xi^{i\ell}) = a\xi^{ir\ell}, \quad i = 0, 1, \dots, (p - 1)/\ell - 1 \geq 2.$$

Taking  $i = 0, 1, 2$  we get  $a = 1$ ,

$$\ell + 1 = \xi^{r\ell} \quad \text{and} \quad 2\ell + 1 = \xi^{2r\ell}$$

which implies

$$(\xi^{r\ell} - 1)^2 = 0.$$

Since  $\gcd(r, (p - 1)/\ell) = 1$ , we get  $\ell = p - 1$ , a contradiction. Finally we have to exclude  $\ell = (p - 1)/2$ . Otherwise we have

$$(p + 1)/2 = f(\xi^{(p-1)/2}) = f(-1) = (-1)^r$$

which is impossible since  $1 < (p + 1)/2 < p - 1$  for  $p > 3$ . Hence,

$$\text{Ind}(f) = p - 1, \quad p > 3.$$

The proof of [9, Theorem 8.2] can be easily adapted to estimate the number  $N$  of solutions of

$$R(c) = \frac{\alpha c + \beta}{\gamma c + \delta} = f(c)$$



in the case  $\gamma \neq 0$ . The case  $\gamma = 0$  follows directly from [9, Theorem 8.2] and gives the bound

$$N(N-1) \leq 2(p-2)$$

which implies

$$\mathcal{L}(f) < (2(p-2))^{1/2} + 1$$

and

$$N < (2(p-2))^{1/2} + 1, \quad \gamma = 0. \quad (15)$$

Now consider the set

$$D = \{2 \leq a \leq p-1 : f(c) = R(c) \text{ and } f(ac) = R(ac) \text{ for some } c\}$$

of size  $|D| \leq p-2$ . There are  $N(N-1)$  pairs  $(c, ac)$ ,  $a \neq 1$ , with

$$f(c) = R(c) \quad \text{and} \quad f(ac) = R(ac) \quad (16)$$

and for some  $a \in D$  (16) has at least  $N(N-1)/|D| > (N-1)^2/(p-2)$  solutions  $c$ . For this  $a$

$$R(ac) = f(ac) = f(c) + d = R(c) + d$$

has either for  $d = f(a) \notin \{0, 1\}$  or for  $d = f(a) - 1 \notin \{-1, 0\}$  at least  $(N-1)^2/2(p-2)$  solutions  $c$ . On the other hand we have

$$R(ac) = \frac{\alpha ac + \beta}{\gamma ac + \delta} = \frac{\alpha c + \beta}{\gamma c + \delta} + d = R(c) + d$$

which implies a quadratic equation for  $c$  since  $ad\gamma \neq 0$  with at most 2 solutions and thus

$$(N-1)^2 \leq 4(p-2), \quad \gamma \neq 0. \quad (17)$$

The case  $\alpha = \delta = 0$  provides the bound on the invertibility  $\mathcal{I}(f)$ . The bound on the Carlitz rank follows by (5), (15) and (17).  $\square$

Finally, we note that the results of this section can be easily extended to arbitrary finite fields using the approach of [14].

## Acknowledgement

The authors are supported by the Austrian Science Fund FWF Projects F5504 and F5511-N26, respectively, which are part of the Special Research Program "Quasi-Monte Carlo Methods: Theory and Applications". L.I. would like to express her sincere thanks for the hospitality during her visit to RICAM. The authors also like to thank Igor Shparlinski for pointing to an improvement of an earlier version of Theorem 1 as well as Alev Topuzoğlu for suggesting earlier research on Carlitz rank which motivated this paper and for all of her kind help.

## References

- [1] E. Aksoy, A.Çeşmelioglu, W. Meidl, A. Topuzoğlu, *On the Carlitz rank of a permutation polynomial*, *Finite Fields Appl.* 15 (2009), 428–440.
- [2] L. Carlitz, *Permutations in a finite field*, *Proc. Amer. Math. Soc.* 4 (1953), 538.
- [3] D. Gomez-Perez, A. Ostafe, A. Topuzoğlu, *On the Carlitz rank of permutations of  $\mathbb{F}_q$  and pseudorandom sequences*, *J. Complexity* 30 (2014), 279–289.
- [4] L. Işık, A. Topuzoğlu, A. Winterhof, *Complete mappings and Carlitz rank*, *Des. Codes Cryptogr.* (to appear).
- [5] R. Lidl, H. Niederreiter, *Finite Fields*. Second edition. *Encyclopedia of Mathematics and its Applications*, 20. Cambridge University Press, Cambridge, 1997.
- [6] G. L. Mullen, D. Wan, Q. Wang, *Index bounds for value sets of polynomials over finite fields*, *Applied algebra and number theory*, 280–296, Cambridge Univ. Press, Cambridge, 2014.
- [7] G. L. Mullen, D. White, *A polynomial representation for logarithms in  $GF(q)$* , *Acta Arith.* 47 (1986), 255–261.
- [8] H. Niederreiter, A. Winterhof, *Cyclotomic  $\mathcal{R}$ -orthomorphisms of finite fields*, *Discrete Math.* 295 (2005), 161–171.

- [9] I. Shparlinski, Cryptographic Applications of Analytic Number Theory. Complexity Lower Bounds and Pseudorandomness. Progress in Computer Science and Applied Logic, 22. Birkhäuser Verlag, Basel, 2003.
- [10] A. Topuzoğlu, *Carlitz rank of permutations of finite fields: a survey*, *J. Symbolic Comput.* 64 (2014), 53–66.
- [11] D. Wan, Q. Wang, *Index bounds for character sums of polynomials over finite fields*, *Des. Codes Cryptogr.* 81 (2016), 459–468.
- [12] Q. Wang, *Cyclotomic mapping permutation polynomials over finite fields. Sequences, Subsequences, and Consequences (International Workshop, SSC 2007, Los Angeles, CA, USA, May 31 - June 2, 2007)*, Lecture Notes in Comput. Sci. 4893, 119–128, Springer, Berlin, 2007.
- [13] Q. Wang, *Cyclotomy and permutation polynomials of large indices*, *Finite Fields Appl.* 22 (2013), 57–69.
- [14] A. Winterhof, *Polynomial interpolation of the discrete logarithm*, *Des. Codes Cryptogr.* 25 (2002), 63–72.